UAV (aka drone) Forensics

Who Am I

David Kovar

- 15+ years of SAR experience
- Fixed wing and rotor pilot
- Big 4:
  - Cyber security investigator
  - Incident response consultant
  - Senior manager

Quadcopter Pilot

What governments think we do

What the media thinks we do

What our partners think we do

What our neighbours think we do

What we think we do

What we really (try) to do

Why Is This Relevant?

Market Growth and Jobs

- CEA forecasts the global market for consumer drones will approach $300 million by 2018 on factory-to-dealer sales of just under a million units. This marks a strong increase over CEA's forecast for 2014 of $84 million in global revenues on sales of 250,000 units.

- AUVSI's *The Economic Impact of Unmanned Aircraft Systems Integration in the United States* report shows the economic benefit of UAS integration. AUVSI's findings show that in the first three years of integration more than 70,000 jobs will be created in the United States with an economic impact of more than $13.6 billion. This benefit will grow through 2025 when we foresee more than 100,000 jobs created and economic impact of $82 billion.

- According to OpenSecrets.org, which tracks the influence of Washington lobbyists, spending by groups pushing for drone legalization has exploded from $35 million in 2011 to $184 million last year

- 10,000 DJI Phantoms sold *each week*.

Illegal and inappropriate activity

- Drug delivery over US/Mexico border
- Drug and weapon delivery to prison
- Multiple invasions of privacy
- Flight above crowds and in controlled airspace
- Flight into operators and bystanders

What You Do?

- Are you in Law Enforcement?
- Agriculture?
- Real estate?
- Mining?
- Oil and Gas?
- Insurance?
- Journalism?
- …

Anti-drone solutions

- RF fingerprinting
- Jamming
- Geo-fencing and no fly zones
- Tangle-drone – Drops net over drone
- Shotguns
- Debris and game jerseys

Terminology

- UAS – Unmanned Aerial System – Emphasis on system
- UAV – Unmanned Aerial Vehicle – The aircraft portion of the system
- GCS – Ground Control Station – The flight control portion of the system. May include manual and automatic control features
- Data link – radio system to transmit data to and from the UAV. Often used for telemetry, sensor data, and FPV operation
- Drone – Common term for any UAV but most often used to describe quads and other multirotor UAVs
- FPV – First Person View – technology that enables the operator to fly the UAV from the perspective of the UAV

Drone Forensics – High Altitude View

DJI Phantom 2 – Example UAV

- Very common UAV
- Relatively easy to hack
- SDK available
- <u>Demonstrates all the major components</u>

What Physical Evidence is Available?

What Digital Evidence is Available?

Physical, digital, and other evidence

Physical

Drone
- Flight controller
- Sensor
- Physical evidence

Ground Station
- Data link
- Ground control station
- Radio controller

Support and Post Processing
- Maintenance system
- Image processing
- Billing, R&D, et al

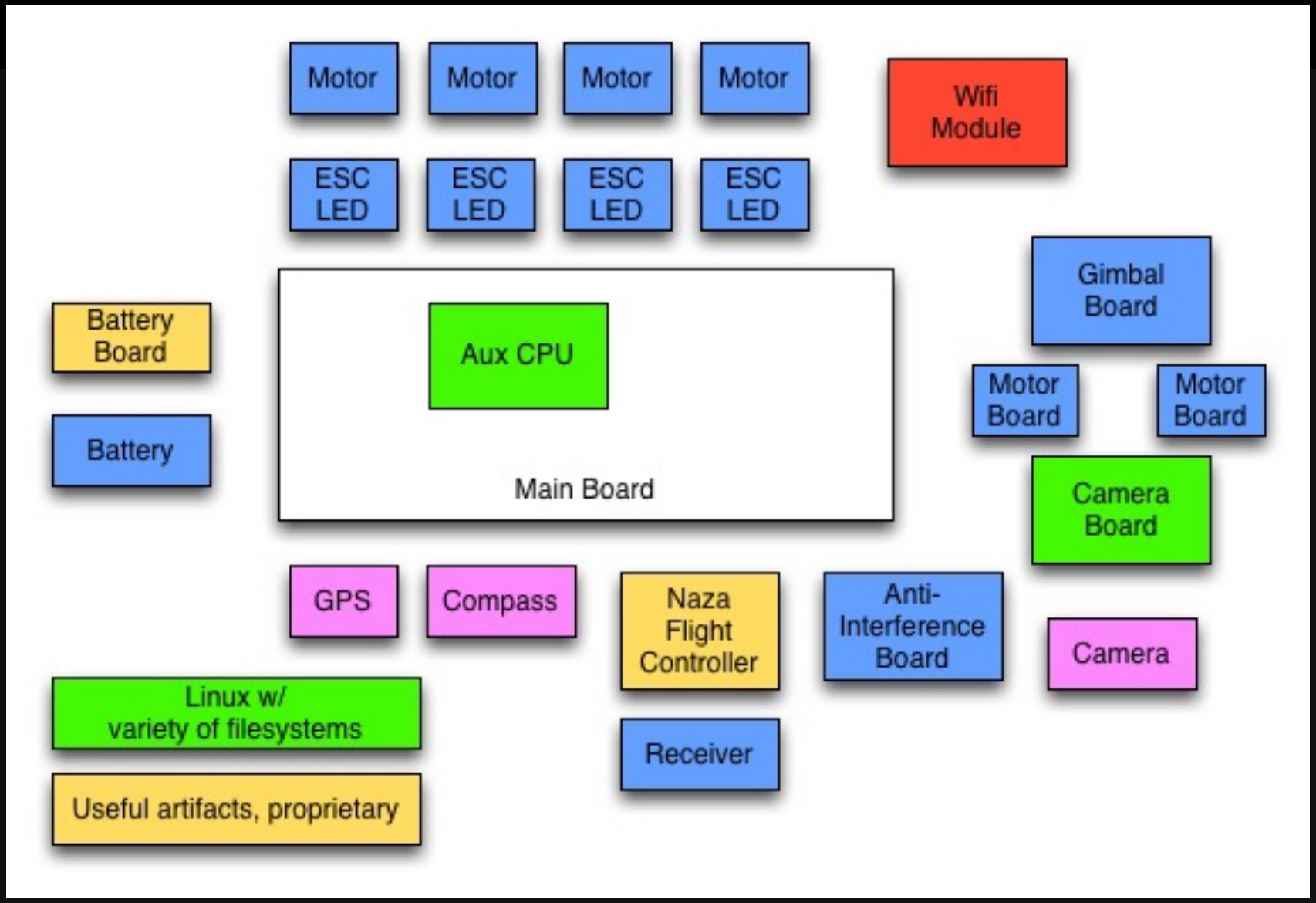
Digital

- Mobile OS
- Traditional OS
- Embedded Linux
- Variety of file systems (e.g. JFFS2)
- Media storage
- EEPROMs
- Firmware

Other

- Mission planning
- Maintenance logs
- Purchase records
- Social media
- Fingerprints

What Is In The UAV



UAV CPUs & “operating systems”

The flight controller is the core system in a UAS and amounts to the aircraft’s CPU & operating system.

Open Source

- Openpilot
- Ardupilot (APM, Pixihawk)
- Multiwii
- KKmultipcopter

Commercial

- Parrot AR Drone FC
- Naza (DJI)
- Wookong (DJI)
- Dualsky (FC450, etc)

- Airware is trying to be the Microsoft/IBM of the UAV world, selling hardware and software that they hope is the defacto standard for flight controllers.
- Linux is the predominant OS for onboard UAV systems

Collection and Analysis Workflow

Workflow

Gather a lot of information

- Systems are highly complex
- Systems can be highly customized
- Lots of components

Determine the problem you are trying to solve

- Crash
- Flight into controlled airspace
- Invasion of privacy
- Illegal activity

Guiding Principles

- **Know what you are looking at**
  - A UAS is just a physical container for a lot of different hardware running a wide array of firmware and software. Determine what everything is before you start trying to analyze anything.
- **Know how to talk to it**
  - USB, WiFi, Bluetooth, physical image, ISP for eMMC, JTAG
- **Know what it is running**
  - OS X, Windows, Linux (embedded or normal), IOS, Android
  - Various small and embedded Linux systems are very common
  - Lots of weird file systems
- **Know what it contains**
  - Are you looking for waypoints, still images, video, configuration files, flight logs ....
- **Know what problem you are trying to solve**
  - Crash, theft, inappropriate use, ...

Forensic Collection Reminders

- Document – form available on my blog
- Photograph – everything – scene, evidence, components, labels, screens
- Fingerprint – If LE
- Mentally break all evidence into component parts – e.g. The UAV probably has removable media on board

We have a crashed drone, now what?

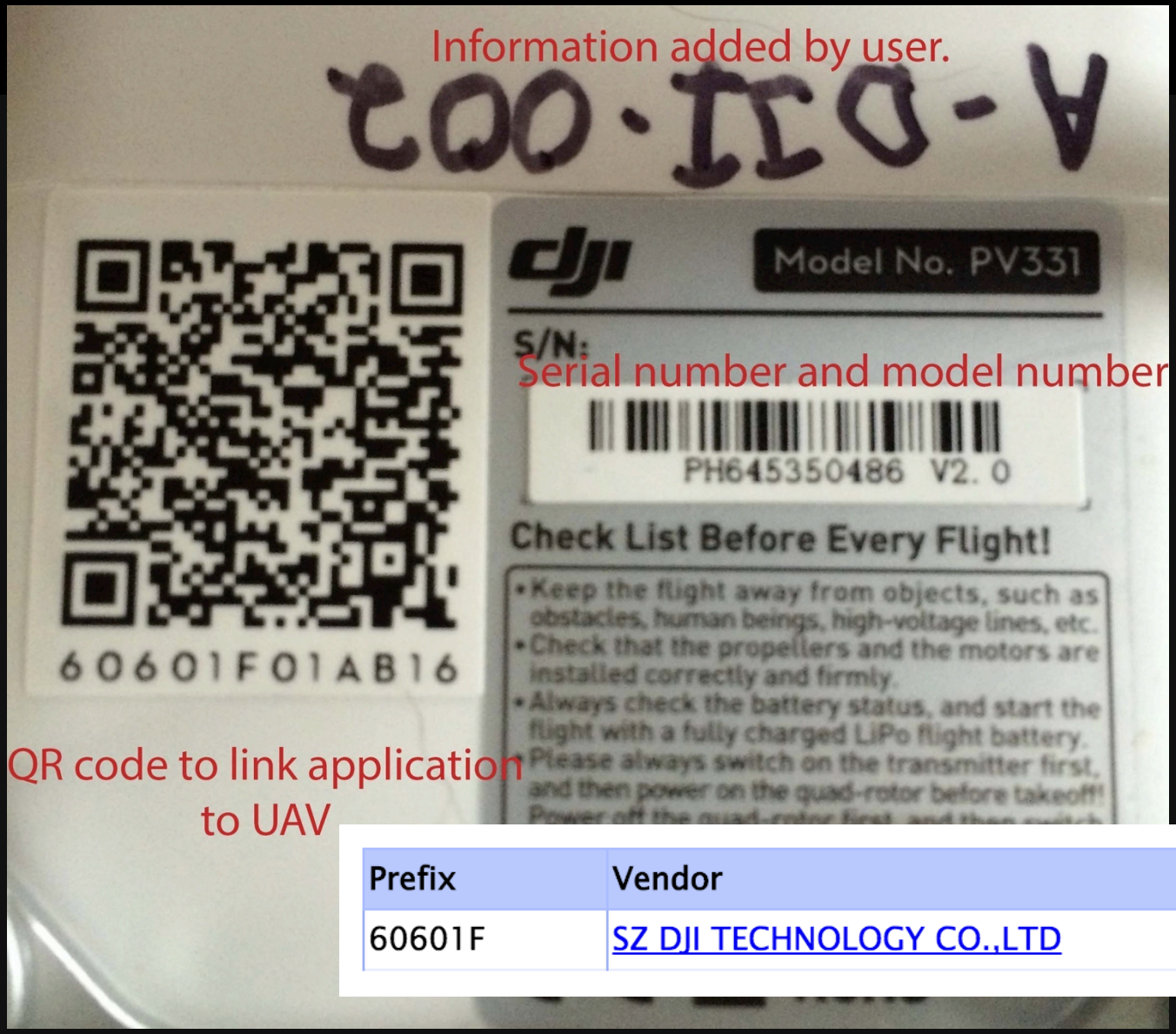
Scenario

The White House lawn was hardly unique

A drone is found on the front yard of a local estate

- **Who owns it?**
- **How did it get there?**
- **Where was it before crashing?**
- **Where was it going?**
- **What was its purpose?**

UAS Exam – UAV



Prefix	Vendor
60601F	SZ DJI TECHNOLOGY CO.,LTD

UAS Exam – DJI QR Code

http://m.dji.net/djivision?1=DJI&2=PHANTOM VISION&3=BH161642215153&4=FC200_01ab16&5=60601F01AB16

- Vendor – DJI
- Model – Phantom 2
- MAC Address - 60601F01AB16

There is a lot of information that you could probably find by fuzzing that URL.

Linux Systems on the DJI Phantom

Connect the Phantom to an OpenWRT AP, connect your analysis system to the AP. Instructions on how to do this available from the web site.

WiFi Extender

(on GCS)

- 192.168.1.2
- root/19881209
- OpenWRT
- Connection point for GCS and analysis systems
- Can be replaced with any OpenWRT system

Camera

- 192.168.1.10
- root/123456

General CPU

- 192.168.1.1
- root/19881209
- Pictures, videos, telemetry
- Mounts camera file system
- Flight controller via ser2net

Collection

```
ssh 192.168.1.1 -l root "dd if=/dev/mem " | dd of=mem.dd
ssh 192.168.1.1 -l root "tar cf - / " | tar xf -
ssh 192.168.1.1 -l root "dd if=/dev/mtdblock3 " | dd of=root.dd
```

Plus a modified copy of Brian Moran's Live Response Collection script for volatile data

Linux Systems - Gotchas

The primary file system on the general purpose CPU is JFFS2 on top of a MTD device. It is also byte swapped. So, to get something you can mount on an analysis system:

Dump the file system:

ssh 192.168.1.1 -l root "dd if=/dev/mtdblock3 " | dd of=root.dd

Then byte swap it:

dd if=root.dd of=root-swap.dd conv=swab

Or apt-get install mtd-utils and do:

jffs2dump -b -c -e dest_file.little src_file.big

This is mounted on top of another file system on the UAV and so to get a complete image you need to dump all of the pieces and reconstruct it.

UAV Exam – SDKs and Live UAV

Most of the flight data is in RAM and most of the flight controller software is running off of flash media. Very little useful data persists after power is removed other than sensor data on the removable media.

Similar to many other “normal” systems, APIs and SDKs exist for UAVs.

Most commercial UAV applications will not extract all of the data an analyst needs.

Be prepared to develop your own investigative tools using SDKs.

UAV Exam – SDKs and Live UAV

Battery: {designedVolume=5200|fullChargeVolume=5200|
currentElectricity=4141|currentVoltage=11876|
currentCurrent=-961|remainLifePercent=100|remainPowerPercent=79|
batteryTemperature=20|dischargeCount=2|}

MC: {satelliteCount=6.0|homeLocationLatitude=40.4314293|
homeLocationLongitude=-89.31180890000002|
phantomLocationLatitude=40.4314619|
phantomLocationLongitude=-89.31181570000001|velocityX=0.0|
velocityY=0.0|velocityZ=-1.0|speed=0.1|
altitude=-8.31500244140625|pitch=0.0|roll=-1.0|yaw=-120.0|
remainPower=11878.0|remainFlyTime=0.0|powerLevel=2.0|
isFlying=false|noFlyStatus=0.0|noFlyZoneCenterLatitude=0.0|
noFlyZoneCenterLongitude=0.0|noFlyZoneRadius=0.0|}

UAV Exam – Data Logging (Black Box)

- Many flight controllers, PixHawk for example, have data logging capabilities included
- Others, such as the DJI Naza, require an off board data logger
- Some ground control station applications have data logging capabilities

The Answer is Often in the Data

Sensor and Sensor Data

- The type of sensor will tell you a lot about the purpose of the flight
  - LIDAR
  - Optical
  - NVIR
  - Thermal
  - WiFi
- The sensor data will tell you a lot about where it has been, particularly since GPS data is critical for most types of missions

Sensors – Optical

Most common sensor out there

- Consumer - GoPro, DJI, Canon, Sony
- Pro-sumer and professional

Artifacts

- The image
- The EXIF data

Location

- Right there on the UAV – pull the SD card

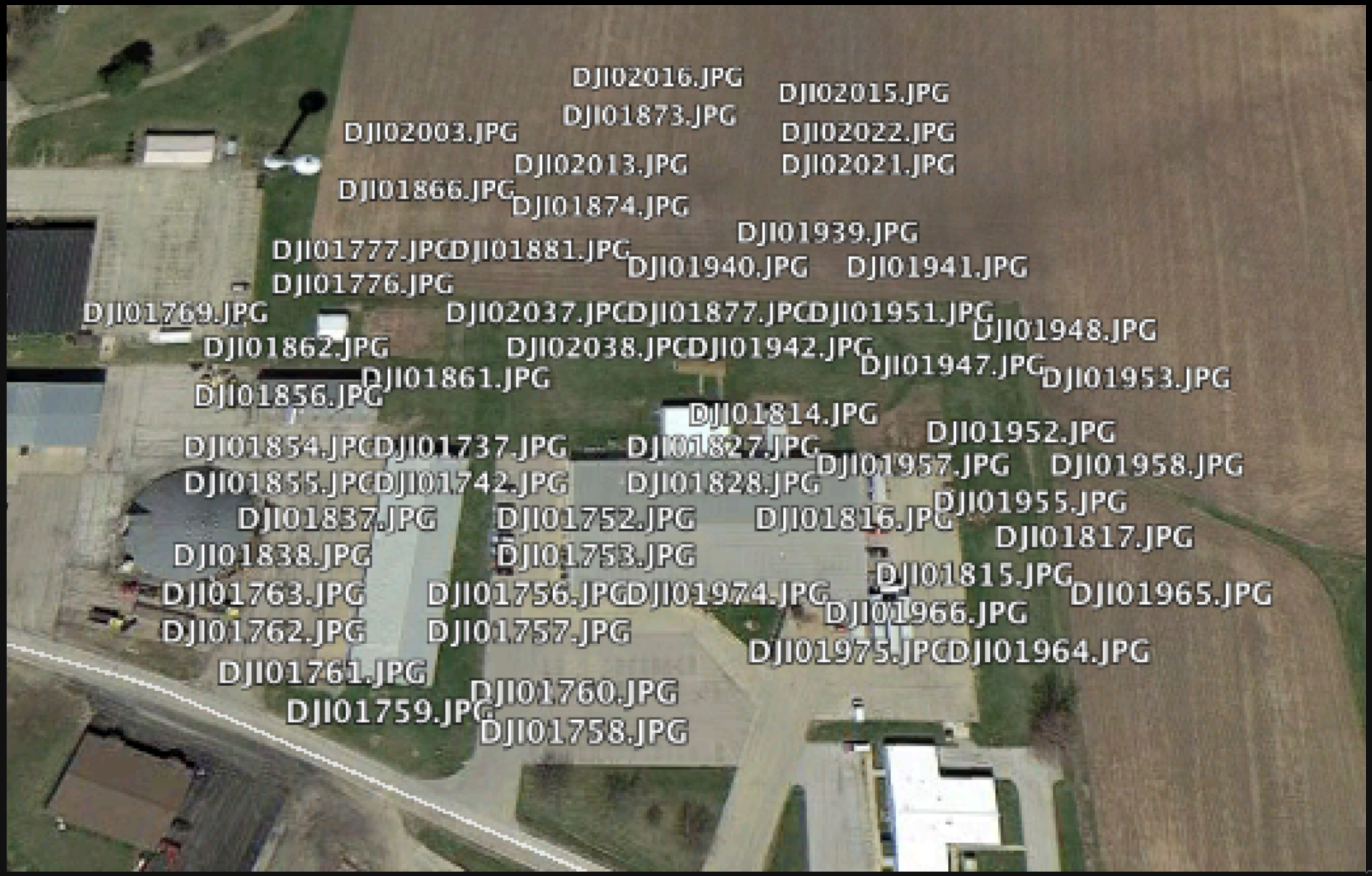
Sensors – EXIF Data

The purpose of a camera is to take a picture, and EXIF data tells a story about the camera and where it was taking pictures.

```
Make                            : DJI
Camera Model Name               : PHANTOM VISION FC200
X Resolution                    : 72
Y Resolution                    : 72
Software                        : Ver.1.0.000
Modify Date                     : 2015:03:21 11:15:23
Date/Time Original              : 2015:03:21 11:15:23
Create Date                     : 2015:03:21 11:15:23
GPS Version ID                  : 2.2.0.0
GPS Latitude Ref                : North
GPS Longitude Ref               : West
GPS Latitude                    : 40 deg 32' 25.00" N
GPS Longitude                   : 89 deg 30' 60.00" W
GPS Position                    : 40 deg 32' 25.00" N, 89 deg 30' 60.00" W
```

DJI Phantoms do not record altitude in the EXIF data unfortunately.

Sensors – EXIF Data



Sensor Data - Cloud

- Consumer
  - YouTube
  - Facebook
  - Etc
- Commercial
  - Data Mapper
  - Airware
  - Vendor specific

Question: Where are the credentials for uploading the imagery data to the cloud?

UAS Exam – Sensor Data

Ah, found the launch point!

UAS Exam – Launch Point Evidence

Ground Control Station

- Often a mobile device combined with a radio controller
- Vendor applications and community developed
- Looking for:
  - Default settings
  - Launch points, dates
  - Owner name, account

Other Items

- Spare removable media
- Other UAVs
- Laptops, cell phones, tablets

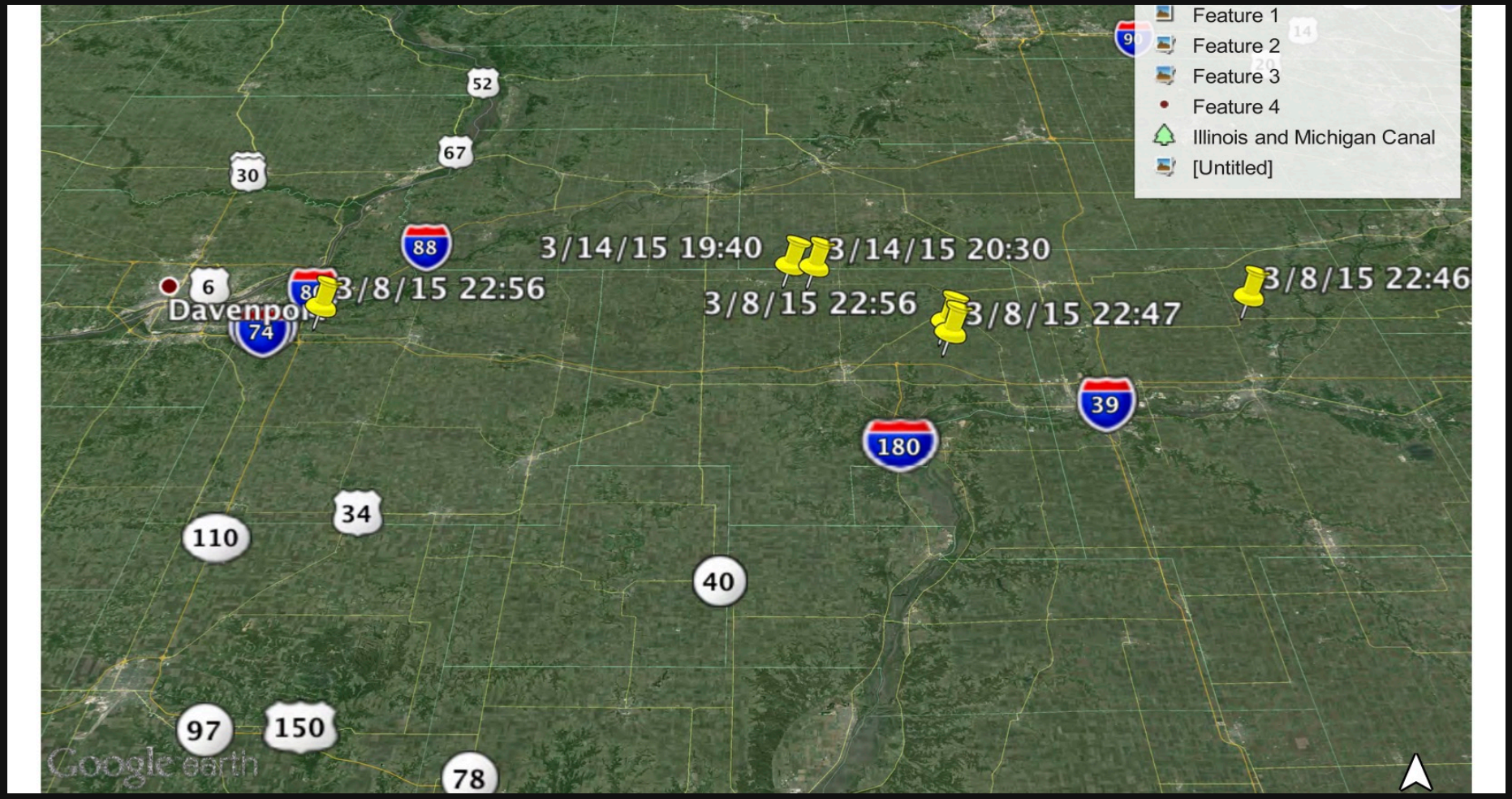
UAS Exam – Ground Control Station

The DJI Vision app records the time and location of the GCS each time it starts up.

ID	flight_time	lat	lng	Date (UTC) (Calculated from flight_time)
1	1425854801	41.481438	-88.811751	3/8/15 22:46
2	1425854820	41.411438	-89.308764	3/8/15 22:47
3	1425855404	41.461562	-90.314724	3/8/15 22:56
4	1425855405	41.431562	-89.311724	3/8/15 22:56
5	1426362056	41.543606	-89.55682	3/14/15 19:40
6	1426365007	41.540626	-89.516805	3/14/15 20:30

UAS Exam – Ground Control Station

Using the data from the GCS, you can rapidly plot where the user was flying.



UAS Exam – Ground Control Station

Application configuration files contain interesting information

```
Path:      /mobile/Applications/com.dji-
innovations.DJEye/Library/Preferences/com.dji-
innovations.DJEye.plist
```

Excerpts

```
email = XXXXXXX@gmail.com; (DJI account information)
password = XXXXXX;

ground_station = 1; (User is flying with waypoints)
fpv_mode = 0;       (User is not flying FPV)
```

UAS Exam – Ground Control Station

Account information leads to useful information on DJI site

Order Number: 001100037932

1 Place Order | 2 Payment Reviewing | 3 Payment Success | 4 Shipped | 5 Order Completed

Payment Status:	Pay Confirmed
Payment Method:	Credit Card
Total:	USD $1[illegible]
Order Time:	2014-12-06 16:41:01
Shipping Address:	[illegible]
Shipping Status:	Recevied
Shipping Company:	FEDEX
Tracking Number:	610[illegible]

My Shipping Address

Contact	Address	Zip Code	Phone
[illegible]	3[illegible]0 Veterans Road Suite [illegible]	61[illegible]	650-[illegible]-1[illegible]74

We’ve traced the UAV back home

UAS Exam – Home & Office Evidence

Maintenance, logging & business systems

- Flight and maintenance logs, often with date/time/location/aircraft
- Client & accounting data

Data analysis system

- If not cloud based, this will have a lot of disk, CPU, and RAM
- Historical sensor data

Other

- UAVs, spare parts
- Spare removable media
- Other GCS

We have a drone in flight, can we do anything?

Scenario – real time

A drone is flying over a local estate

- Who is flying it?
- Where is it going?
- What is it collecting?

Can we answer these questions?

Yes

Real Time Analysis

Connect via WiFi and send commands to the flight controller using ser2net.

```
** Rcv from port 0x08, seq     0, cmd 0x04, subcmd 0x00, error 0,
payload len  0

0x0400: server says hello!

** Sent to  port 0x0a, seq     3, cmd 0x53, subcmd 0x00, error 0,
payload len  0

** Rcv from port 0x0a, seq     2, cmd 0x49, subcmd 0x00, error 0,
payload len  52

[0x49]: Seq     2, GPS sats 4, home [+40.431455, -89.311694] loc
[+40.431496, -89.311653], accel xyz [+00, +00, +00], ag +1.2 meter,
compass roll/pitch/heading [180, 180, 093], batt 12065mV (74%),
unknown 6

[0x53]: Seq     3, battery <5200mA, 5440mA>, current level <12090mV,
4619mA>, unknown 6e fc 63 54 1e 03 00
```

Real Time Hijack of UAV

Several commercial UAVs use WiFi for command & control and data. A user can identify the SSID, deauthenticate the UAV, and then capture the UAVs attempt to reestablish the link. Once the link is established, they can control the UAV, download telemetry, or download sensor data.

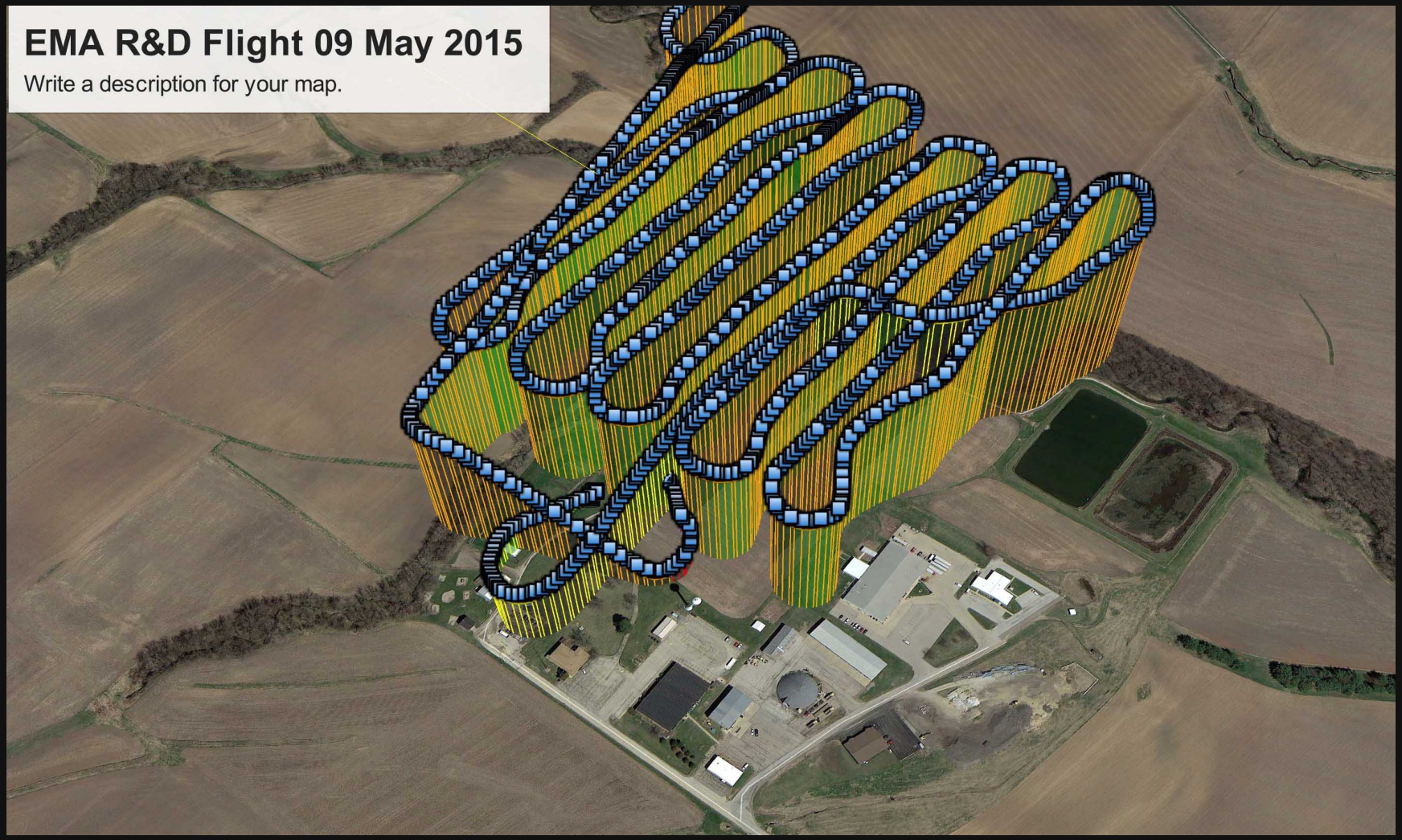
Skyjack is a AR Parrot hijack tool. This approach will work on a DJI Phantom using WiFi as well.

You can hack into other data link mechanisms as well.

Analysis of Other UAVs

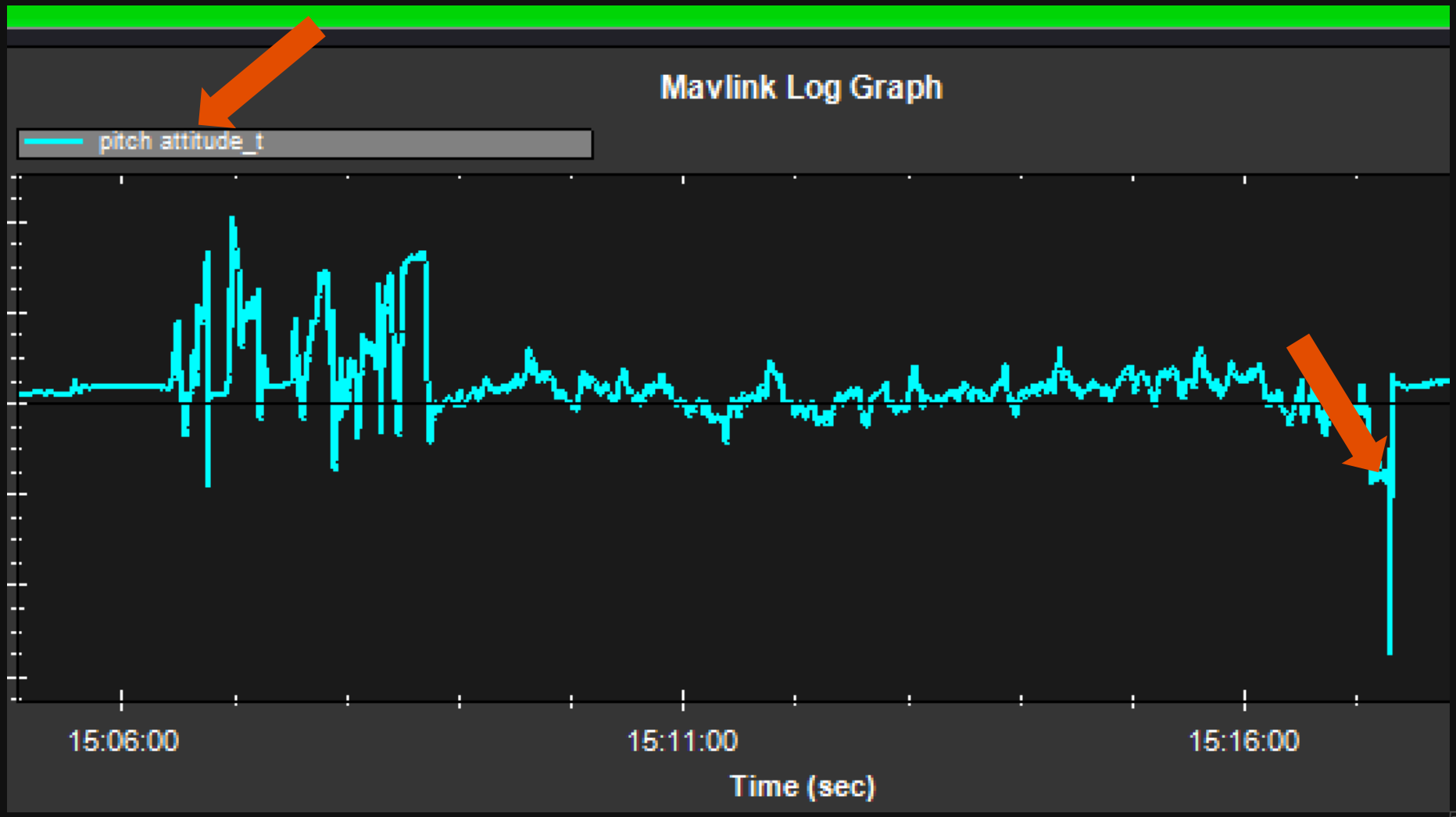
UAVs with PixHawk Flight Controller

The following was created in under two minutes using Mission Planner



UAVs with PixHawk Flight Controller

And this is what a crash looks like ....



UAVs with PixHawk Flight Controller

And all flight parameters are easily collected

```
FS_BATT_MAH      0
MIS_RESTART      0
AFS_WP_COMMS     0
INS_ACCOFFS_Z    -0.3554053
AFS_ENABLE       0
RLL2SRV_I        0.1
PTCH2SRV_TCONST  0.5
EKF_WIND_PNOISE  0.1
RNGFND_OFFSET    0
BATT2_MONITOR    0
FBWB_ELEV_REV    0
TERRAIN_ENABLE   1
ALT_HOLD_RTL     10000
ELEVON_OUTPUT    0
ARMING_REQUIRE   0
RLL2SRV_D        0.1
RCMAP_PITCH      2
EKF_GYRO_PNOISE  0.015
SR0_EXTRA3       2
AFS_TERM_PIN     -1
RELAY_DEFAULT    0
SR0_POSITION     3
AUTO_FBW_STEER   0
ALT_OFFSET       0
TECS_LAND_ARSPD  -1
FORMAT_VERSION   13
BATT2_VOLT_PIN   2
AHRS_GPS_MINSATS         6
RALLY_TOTAL      0
RC1_DZ   30
```

Closing Thoughts

Challenges & Solutions

- Data and command & control moving from WiFi to Bluetooth to dedicated radio to LTE & 4G
    - Harder to hack, easier to triangulate and identify with existing tools
- Many vendors, lots of variety, embedded systems
- Focus on ground control stations and post processing systems, analyze the sensor data. They tell 80% of the story

Closing Thoughts - Forensics

The UAV is paired with controller

And

The UAV is also paired with ground control station

Means unique IDs

Means forensic evidence linking devices

Closing Thoughts - Forensics

I needed to analyze the following to cover the entire system:

- Three different versions of Linux
- IOS or Android
- OS X or Windows
- 6+ file systems
- ser2net
- Wifi or Bluetooth or 915Mhz data link
- EXIF
- GPS
- “Social media”
- SDK

No single UAV analysis tool

Closing Thoughts

Cybersecurity:

The proper term for drones is sUAS – small unmanned aerial system. Take a system approach to security and investigations, do not treat the vehicle as a discreet or standalone element.

Law & Policy:

UAVehicle. Apply law and policy to the risk/threat posed by the sensors and services rather than by the delivery mechanism

Wrap Up

PLEASE contact me with questions, pointers, suggestions.

- dkovar@kovarllc.com
- @dckovar